ABSTRACT

The present invention provides a configuration capable of effectively preventing an encrypted content stored on an information-recording medium from being misused. In this configuration, a seed (seed 2) required for generating a block key to be applied to a process to decode an encrypted content is stored as information encrypted by using another block key Kb1. In addition, in a configuration where the seed (seed 2) needs to be transferred from a device to another, both the seed (seed 2) and a recording key K2 are transferred from the device to the other as information encrypted by using a session key. In such configurations, it is difficult to analyze the seed (seed 2) by acquisition of data from the information-recording medium or a data transmission line. Thus, difficulties to analyze a key generated by using the seed and analyze an encryption algorithm are increased. As a result, protection of contents at a high level of security can be implemented.